DOCKET NO.: 13608ROUS02U

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Donald R. HORNE

SERIAL NO:	09/996,671	ART UNIT:	2182
FILED:	November 30, 2001	EXAMINER:	Unknown

SUBJECT: MANAGEMENT OF LOG ARCHIVAL AND REPORTING FOR DATA NETWORK SECURITY SYSTEMS

ATTENTION: Jon Lachei - Pre-Grant Publications Division

#7

THE ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231, U.S.A.

Sir:

REQUEST FOR CORRECTED APPLICATION PUBLICATION

This request is filed in respect of the above-referenced application to correct material errors in **Application Publication No. US-2002-0138762-A1** dated September 26, 2002.

Upon review we noted that between paragraph [0133] and [0134] of the published application, a section of the application from page 22, line 5 to page 41, line 30 of the original application is entirely missing. Copies of the missing pages of the application as filed are transmitted herewith.

The Commissioner is hereby authorized to charge any fees which may be required, or credit and overpayment to **Deposit Account No. 14-1315.**

Yours very truly,

Donald R. HORNE

By Angela C. de Wilton

Angela C. de Wilton,
Patent Agent
Registration. No. 35,763

ACdW/jo:Encls.
c/o NORTEL NETWORKS LIMITED
Intellectual Property Law Group
P.O. Box 3511, Station "C"
Ottawa, Ontario, Canada K1Y 4H7

Phone: (613) 768-3020
FAX: (613) 768-3017

Date: November 27, 2002

Components Inputs and Outputs

This section provides further details of the component inputs and outputs used in the system according to the embodiment.

Log Collector (LC)

Input from LCM:

System_configuration

Retrieval_Interval={default=24 hrs | hourly interval=1 - 24 hrs}

Cleanup_Interval={ default=7 days | weekly interval=1 - 7days)

Output to LCM:

Log transfer list

LC_Name {FQHN, IP address}

SD_Name {FQHN, IP address}

Date

Retrieval_Interval

Time

Files={file1, file2, file3...)

Errors

file 1

file 2

file 3

Log Collector Manager (LCM)

Input from DAM:

System_configuration

Retrieval_Interval={default=24 hrs | hourly interval=1 - 24 hrs}

Cleanup_Interval={ default=7 days | weekly interval=1 - 7days)

LC_List={LC_Name1, LC_Name2, LC_Name3...)

```
            LC_Name 'n'={FQHN, IP address}
                 SD_List={SD_Name1, SD_Name 2, SD_Name
3...)
                      SD_Name 'n'={FQHN, IP address}
    LCM_status_request /* request status update of LC
log archiving managed by LCM */

Input from LC:
     Log transfer list
          LC_Name {FQHN, IP address}
          SD_Name {FQHN, IP address}
          Date
          Retrieval_Interval
          Time
          Files={file1, file2, file3...)
          Errors
     file 1
     file 2
     file 3

Output to SM:
     Log transfer list
          LCM_Name {FQHN, IP address}
          LC_Name {FQHN, IP address}
          SD_Name {FQHN, IP address}
          Date
          Retrieval_Interval
          Time
          Files={file1, file2, file3...)
     file 1
     file 2
     file 3

Output to DAM:
```

Log archival transaction complete
LCM_Name {FQHN, IP address}
LC_Name {FQHN, IP address}
SD_Name {FQHN, IP address}
Errors
LCM_archival_complete /*when all logs have been transferred to the SM for that interval*/
LCM_status_update
LC_List={LC_Name1, LC_Name2, LC_Name3...}
LC_Name'n'={FQHN, IP address, status=[archived | cached |waiting]}

Storage Manager (SM)

Input from LCM:

Log transfer list
LCM_Name {FQHN, IP address}
LC_Name {FQHN, IP address}
SD_Name {FQHN, IP address}
Date
Retrieval_Interval
Time
Files={file1, file2, file3...}
file 1
file 2
file 3

Input from DAM:

System_configuration
Archival_Duration={type1, type2, type3...}
type'n'={online=[number_months], offline=[number_months]}
Log_Location_Request
SD_Type
SD_Name {FQHN}

```
            Date
            ONLINE-OFFLINE_bit /* bit 'on' when auto
analysis is being done on newly arrived logs */
            Filepath_List={filepath1, filepath2,
filepath3...} /* file path given for restored offline
logs */
      Log_Info_Request
            SD_Type
            SD_Name {FQHN}
            Date
      Online_Table_Request
      Offline_Table_Request

Output to DAM:
      Log_Location_Reply
            SD_Type /* type derived from name */
            SD_Name {FQHN, IP address}
            Date
            Retrieval_Interval
            Time
            File_Location_List={filepath1, filepath2,
filepath3...}
                  filepath'n'={ONLINE_bit, ONLINE=filepath}
      Log_Info_Reply
            SD_Type
            SD_Name {FQHN, IP address}
            LCM_Name
            LC_Name
            Online_Offline
            Offline_Date
            Online_Date
            Log_Date
            Retrieval_Interval
      Online_Table_Reply
```

Offline_Table_Reply

Online Log Archival Table

SD_Type

SD_Name

IP_address

LCM_Name

LC_Name

Archival_Date

Log_Date

Retrieval_Interval

Time={time1, time2, time3...}

Filepath={filepath1, filepath2, filepath3...}

Offline Log Archival Table

SD_Type

SD_Name

IP_address

LCM_Name

LC_Name

Offline_Date

Log_Date

Retrieval_Interval

Time={time 1, time2, time3}

Filepath={N/A, N/A, N/A}

Data Analysis Manager (DAM)

Input from LCM:

Log archival transaction complete

LCM_Name {FQHN, IP address}

LC_Name {FQHN, IP address}

SD_Name {FQHN, IP address}

Errors

```
        LCM_archival_complete /*when all logs have been
    transferred to the SM for that interval*/
        LCM_status_update
            LC_List={LC_Name1, LC_Name2, LC_Name3...}
                LC_Name'n'={FQHN, IP address,
    status=[archived | cached |waiting]}

    Input from WAS:
        Log_Location_Request /* for custom analysis */
            SD_Type
            SD_Name {FQHN, IP address}
            Date_Range={Date | From_To}
            Online={ONLINE | OFFLINE}
            Offline_File_Location_List={filepath1,
    filepath2, filepath3...}/* restored filepath known */
            FULL_TEXT={ON | OFF}
        Custom_Metrics_Request
            Filter_Type={customized filter keys}
            SD_Type
            SD_Name {FQHN}
            Date_Range={Date | From_To}
        Online_Table_Request
        Offline_Table_Request

    Input from SM:
        Log_Location_Reply
            SD_Type
            SD_Name {FQHN, IP address}
            Date
            Retrieval_Interval
            Time
            File_Location_List={filepath1, filepath2,
     filepath3...}
                filepath'n'={ONLINE_bit, ONLINE=filepath}
```

Log_Info_Reply
SD_Type
SD_Name {FQHN, IP address}
LCM_Name
LC_Name
Online_Offline
Offline_Date
Online_Date
Log_Date
Retrieval_Interval
Online_Table_Reply
Offline_Table_Reply

Input from DAS:
System_Configuration
Archival_Duration={type1, type2, type3...}
type'n'={online=[number_months], offline=[number_months]}
Retrieval_Interval={default=24 hrs | hourly interval=1 - 24 hrs}
Cleanup_Interval={ default=7 days | weekly interval=1 - 7days}
SDtypes={type1, type2, type3...}
type'n'={code, description}
Devicelist={device1, device2, device3...}
Filters={filtertype1, filtertype2, filtertype3...}
filtertype'n'={key1, key2, key3...}
Alarms={alarmtype1, alarmtype2, alarmtype3...}
alarmtype'n'={key1, key2, key3...}
LCMlist={lcm1, lcm2, lcm3...}
lcm'n'={FQHN, IPaddr, responsibility}

Output to LCM:

SD system configuration file:

Retrieval_Interval={default=24 hrs | hourly interval=1 - 24 hrs}

Cleanup_Interval={ default=7 days | weekly interval=1 - 7days}

LC_List={LC_Name1, LC_Name2, LC_Name3...}

LC_Name 'n'={FQHN, IP address}

SD_List={SD_Name1, SD_Name 2, SD_Name 3...}

SD_Name 'n'={FQHN, IP address}

LCM_status_request /* request status of LC log archiving managed by LCM */

Output to SM:

System_Configuration

Archival_Duration={type1, type2, type3...}

type'n'={online=[number_months], offline=[number_months]}

Log_Location_Request

SD_Type

SD_Name {FQHN}

Date

ONLINE-OFFLINE_bit /* bit 'on' when auto analysis is being done on newly arrived logs */

Filepath_List={filepath1, filepath2, filepath3...}

Log_Info_Request

SD_Type

SD_Name {FQHN}

Date

Online_Table_Request

Offline_Table_Request

Output to WAS:

```
        Full_Text_Reply
             Logfile_Text_Buffer /* for read-only access */
        Custom_Metrics_Reply
             Metrics_Table
                  Status
                  Errors
                  Alarms
                  Search_Results
        Online_Table_Reply /* summary of logs archived
online */
        Offline_Table_Reply /* summary of logs archived
offline */

    Output to DAS:
        Session_Analysis
             Date={Month, Day, Year}
             Start_Time
             Session_ID
             Device_Type
             Logfile_Type
             Logfile_Date_Time
             Retrieval_Interval
        Session_Results
             Date={Month, Day, Year}
             Completion_Time
             Session_ID
             Device_Type
             Logfile_Type
             Logfile_Date_Time
             Error_Code
             Alarms={none | [alarm1, alarm2, alarm3...]}
             Errors={none | [error1, error2, error3...]}
             Metrics={key1results, key2results,
key3results...}
```

key'n'results={hit1, hit2, hit3...}

Device_Update

Device_Type

Device_Name

Status={ACTIVE, HISTORIC}

Data Analysis Store (DAS)

Database Schema

TABLE: analysis_session (used to store information about the logfile analysis)

FIELDS:

session_id /* incorporate the date into the sessionid */

year /* Required for */

month /* ease of extraction of */

day /* summary metrics.*/

device_type (name of firewall contivity switch, spam machine,...)

logfile_type (type of file that was parsed. ie. some SDs will produce a number of logfiles)

logfile_date (date and time of logfile)

retrieval_interval (system log retrieval rate)

start_time /* required to track DAM-system */

completion_time /* performance */

TABLE: session_alarms

FIELDS:

session_id

alarmcode

status /* status of each alarm - active or acknowledged */

severity

TABLE: session_errors

FIELDS:

session_id

errorcode

status /* status of each error - active or acknowledged */

severity

TABLE: logfile_types (used to store information about versions of software e.g., firewall - Raptor 4.0 vs Raptor 6.0)

FIELDS:

device_type

logfile_type

TABLE: metric_types (used to store information about the metrics that need to be calculated and where to find the results)

FIELDS:

metric_id (this will be a number from 1 - 30 and is the place where the results are stored in the tables. For example, if this has a value of 2, then in the individual results tables the result of this metric is stored in the metric2 field.)

device_type (ie. FIREWALL,SPAM,CONTIVITY,FTPDROPBOX,USER_STATS)

logfile_type (e.g. Raptor 4, Raptor 6)

metric_name (this is the name that is used to describe the particular metric being found ie. Number of FTP connects)

metric_key (this is the value that is being searched ie. ftp.*connection for)

status (as we are storing all metrics for many years in the database, a particular metric that was used in the past may no longer be valid but still requires a placeholder in the database for historic data. The possible entries in this field are ACTIVE, or HISTORIC where if the status is ACTIVE, then it will be used for analysis)

TABLE: user_table (used to store information about the users accessing this tool)

FIELDS:

userid (ie. CN for certs or userid)

device_type (i.e. ALL,FIREWALL,SPAM,CONTIVITY,FTPDROPBOX,USER_STATS)

type_of_access (e.g. DBA, ANALYST, HELPDESK, CORP-INVESTIGATIONS)

user_name

user_phone

TABLE: access (used to store information about the different levels of access)

FIELDS:

type_of_access (e.g. DBA, ANALYST, HELPDESK, CORP-INVESTIGATIONS)

TABLE: special_access (used to determine access rights to a log in scenarios where specific, limited access is granted)

FIELDS:

userid (ie. CN for certs or userid)

device_name (i.e. ALL, FQHN(S)) /* required for security investigations */

date (i.e. ALL, DATE RANGE) /* required for security investigations */

TABLE: firewall (used to store the metrics gathered on a per firewall basis per logfile basid - for the first cut there will be one entry per firewall per day but as the processing becomes more often, there may be many per firewall per day.)

FIELDS:

session_id

metric1 to metric 30 (used for counts and sums)

TABLE: firewall_monthly (used to store firewall information but summarized by month)

FIELDS:

firewall

year

month

metric1 to metric 30

TABLE: firewall_user (used to store firewall information based on the USER_STATS)

FIELDS:

transaction_type - things like connects per userid, bytes transferred per userid, etc. This information is done on a per firewall per logfile basis)

session_id

userid

metric1 to metric 30

TABLE: firewall_keyword (used to store the matched keyword information. This is done on a per firewall per logfile basis.)

FIELDS:

session_id

search_key

matched_line (string where the match was found)

userid (if possible, the userid extracted from the matched line)

count(?) (ongoing count rather than additional entries in the db?)

TABLE: contivity (used to store the metrics gathered on a per contivity basis per logfile basis)

FIELDS:

session_id

metric1 to metric 30 (counts and sums)

TABLE: contivity_monthly (used to store contivity information but summarized by month)

FIELDS:

contivity

year

month

metric1 to metric 30

TABLE: contivity_user (used to store contivity information based on the USER_STATS)

FIELDS:

transaction_type (things like connects per userid, bytes transferred per userid, etc. this information is done on a per contivity per logfile basis)

session_id

userid

metric1 to metric 30

TABLE: contivity_keyword (used to store the matched keyword information. This is done on a per contivity per logfile basis.)

FIELDS:

session_id
search_key
matched_line (string where the match was found)
userid (if possible, the userid extracted from the matched line)
count(?) (ongoing count rather than additional entries in the db?)

TABLE: dropbox (used to store the metrics gathered on a per dropbox basis per logfile basis)

FIELDS:
session_id
metric1 to metric 30

TABLE: dropbox_monthly (used to store dropbox information but summarized by month)

FIELDS:
dropbox
year
month
metric1 to metric 30

TABLE: dropbox_user (used to store firewall information based on the USER_STATS)

FIELDS:
transaction_type - things like connects per userid, bytes transferred per userid, etc. this information is done on a per dropbox per logfile basis)
session_id
userid
metric1 to metric 30

TABLE: dropbox_keyword (used to store the matched keyword information. This is done on a per firewall per logfile basis.)

FIELDS:

session_id

keyword_key (key that was looked for)

matched_line (string where the match was found)

userid (if possible, the userid extracted from the matched line)

count(?) (ongoing count rather than additional entries in the db?)

TABLE: list_contivity (used to store the list of contivities that have information stored in this database)

FIELDS:

device_status (as we are storing metrics for many contivities for many years in the database, a particular contivity that was used in the past may no longer be valid but still requires a placeholder in the database for historic data. The possible entries in this field are ACTIVE, or HISTORIC where if the status is ACTIVE, then it will be used for analysis)

device_name

logfile_type

TABLE: list_dropboxes (used to store the list of dropboxes that have information stored in this database)

FIELDS:

device_status (as we are storing metrics for many dropboxes for many years in the database, a particular dropbox that was used in the past may no longer be valid but still requires a placeholder in the database for historic data. The

possible entries in this field are ACTIVE, or HISTORIC where if the

status is ACTIVE, then it will be used for analysis)

device_name

logfile_type

TABLE: list_firewalls (used to store the list of firewalls that have information stored in this database)

FIELDS:

device_status (as we are storing metrics for many firewalls for many years in the database, a particular firewall that was used in the past may no longer

be valid but still requires a placeholder in the database for historic data. The possible entries in this field are ACTIVE, or HISTORIC where if the status is

ACTIVE, then it will be used for analysis)

device_name

logfile_type

TABLE: list_keywords (used to store the list of keywords that are to be used as part of an analysis)

FIELDS:

search_key (search string)

device_type

logfile_type

responsibility (group who supplied the keyword and is responsible to investigate when found - HR (Human Resources), NS (Network Security), CS

(Corporate Security))

status (as we are storing metrics for many firewalls for many years in the database, a particular firewall that was used in the past may no longer be valid

but still requires a placeholder in the database for historic data. The possible entries in this field are ACTIVE, or HISTORIC where if the status is ACTIVE, then it will be used for analysis)

TABLE: mailshield (used to store mailshield metrics)

FIELDS:

session_id

metric1 to metric 30 (sum and counts)

logfile_type

TABLE: spam_rejections (used to store top 10 rejection types)

FIELDS:

session_id

reject1 to reject10

occurrence1 to occurrence10

TABLE: list_mailshields (used to store the list of mailshields that have information stored in this database)

FIELDS:

device_status (as we are storing metrics for many mailshields for many years in the database, a particular mailshield that was used in the past may no longer be valid but still requires a placeholder in the database for historic data. The possible entries in this field are ACTIVE, or HISTORIC where if the status is ACTIVE, then it will be used for analysis)

device_name

TABLE: mailshield_monthly (used to store mailshield information but summarized by month)

FIELDS:

mailshield

year

month

metric1 to metric 30

TABLE: blocked (used to store blocked metrics)

FIELDS:

session_id

recipient_emailid

reason (store the reason that the email was blocked)

subject (the subject of the blocked email)

sender

TABLE: owners

FIELDS:

responsibility (ie, HR (Human Resources, NS (Network Security), CS (Corporate Security))

contact_name (person to contact when matched)

userid

contact_phone

contact_email (This is key so that an email can be sent out, assuming we decide to automate this function)

TABLE: error_list (used to store information about possible system errors)

FIELDS:

errorno

severity

description

TABLE: alarm_list (used to store information about log alarms)

FIELDS:

alarmcode

severity

description

TABLE: device_types (used to store list of valid device_types - these will be hard-coded into this table)

FIELDS:

device_type (i.e. FIREWALL, CONTIVITY, SPAM,...)

TABLE: lcm_list (used to store list of Log Collector Managers)

FIELDS:

device_name

responsibility (string - depending on implementation could be geographic or device type dependent)

TABLE: sys_config (used to store list of system parameters)

FIELDS:

retrieval_interval

cleanup_interval

device_type

online_duration

offline_duration

Intellectual Property Law Group
P.O. Box 3511, Station C
Ottawa, Ontario, Canada
K1Y 4H7

NORTEL NETWORKS
How the world shares ideas.

Fax Cover Sheet

Date	November 27, 2002		
To	Jon Lachel Pre-Grant Publications Division U.S. PATENT & TRADEMARK OFFICE	**From**	Angela C. de Wilton Nortel IP Law Group
Fax #	(703) 305-8568	**Fax #**	613-768-3017
Phone #	(703) 605-4285-	**Phone #**	613-768-3020
No. of Pages To Follow	21		

Message

Re: U.S. Patent Application Serial No. 09/996,671
Docket No.: 13608ROUS02U

Please see attached Request for Corrected Application Publication.

CERTIFICATE OF FACSIMILE TRANSMISSION

I hereby certify that this correspondence is being facsimile transmitted to the Patent and Trademark Office, Fax No. **703-305-8568** on the date shown below.

Joanne Ohmayer ..... Nov. 27, 2002
Signature Date

Joanne Ohmayer (613-768-3005), Facsimile Operator for this transmission
Nortel Networks Corporation, Intellectual Property Law Group

Treatment of Originals:

___X___ Retained on File _____ Sent by Post _____ Sent by Courier

For enquiries about this transmission, please call Joanne Ohmayer at (613) 768-3005 (ESN 398)